НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК 519.21

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“15” травня 2018р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика»

на тему: Алгебраїчні методи виявлення прихованих фейстель-подібних структур

Виконав (-ла): студент (-ка) 2 курсу, групи _____ФІ-63М_____
(шифр групи)

Оксьоненко Максим Петрович

Керівник к.т.н. Яковлєв С.В.

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент к.т.н. Харченко К.В.

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018року

РЕФЕРАТ

Кваліфікаційна робота містить: 41 сторінку, 11 рисунків, 10 джерел.

Обєктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є схеми $MISTY$ та R-схема.

В роботі проводиться уточнення методів виявлення прихованих аналітичних структур, зокрема фейстель-подібних перетворень, за допомогою індикаторної матриці високого порядку.

Показано, який вигляд має індикаторна матриця високого порядку для схем $MISTY$ та R-схем в залежності від кількості раундів та алгебраїчного степеня раундової функції.

БЛОЧНИЙ ШИФР, БУЛЕВА ФУНКЦІЯ, МЕРЕЖА ФЕЙСТЕЛЯ, ІНДИКАТОРНА МАТРИЦЯ ВИСОКОГО ПОРЯДКУ

РЕФЕРАТ

Квалификационная работа содержит: 41 страницу, 11 иллюстраций, 10 источников литературы.

Объектом исследования являются информационные процессы в системах криптографической защиты.

В работе проводится уточнение методов обнаружения скрытых аналитических структур, в частности фейстель-подобных преобразований, с помощью индикаторной матрицы высокого порядка.

Показано, какой вид имеет индикаторная матрица высокого порядка для схем $MISTY$ та R-схем в зависимости от количества раундов и алгебраической степени раундовой функции.

БЛОЧНЫЙ ШИФР, БУЛЕВАЯ ФУНКЦИЯ, СЕТЬ ФЕЙСТЕЛЯ, ИНДИКАТОРНАЯ МАТРИЦА ВЫСОКОГО ПОРЯДКА

ABSTRACT

The thesis consists of 41 pages, 11 figures, 10 sources.

The object of research is the information processes in cryptographic protection systems.

The subject of specification for detection of hidden analytical structures, in particular Feistel-like networks with the help of High-Degree Indicator matrix.

We show the kind of High-Degree Indicator matrix depending on number of rounds and algebraic degree of round function.

BLOCK CIPHER, BOOLEAN FUNCTION, FEISTEL NETWORK, HIGH-DEGREE INDICATOR MATRIX

ЗМІСТ

ВСТУП

Актуальність роботи. На сучасному етапі розвитку суспільства однією з найбільших цінностей стала інформація. Важливим питанням на сьогоднішній день є захист інформації. Існує декілька напрямків та підходів до захисту інформації, і один із них це криптологія, тобто захист математичними методами. Розвиток електронно-обчислювальної техніки та математичного апарату дає зловмисникам все більше можливостей для дешифрування інформації. З плином часу до алгоритмів шифрування висуваються все більш суворі вимоги, а кожний новий запропонований метод перевіряється все більш детально на велику кількість вразливостей.

Одним із найпоширеніших методів криптографічного захисту конфіденційності інформації є блочні симетричні шифри. На сьогодні відомо багато таких шифрів, які щодня захищають велику кількість інформації. Тому питання про їхню стійкість турбує криптографічну спільноту й є як ніколи актуальним.

Одним із найпоширеніших методів побудови блочних шифрів є мережі Фейстеля. Це ітеративна раундова структура, яка складається з комірок Фейстеля. На вхід кожній комірці подаються дані й ключ. Мережі Фейстеля набули популярності через те, що вони можуть бути доволі легко реалізовані апаратно чи програмно й мають гарні криптографічні властивості. Велика кількість сучасних блочних шифрів (DES, $RC2$, $RC5$, $RC6$, $Blowfish$, $FEAL$, $CAST$-128, TEA, $XTEA$, $XXTEA$) побудовані на основі мереж Фейстеля або їх узагальнених модифікацій.

В зв'язку з такою популярністю з'явились деякі різновиди мереж Фейстеля ($MISTY$, R-схема), які можуть відрізнятися складністю реалізації та криптографічними властивостями. Знайдено методи, які дозволяють розпізнавати звичайні фейстелівські перетворення на основі обчислення для них індикаторних матриць високого порядку. У

відкритому доступі не було знайдено подібних досліджень для інших фейстель-подібних перетворень, зокрема для схеми $MISTY$ та R-схеми.

Мета та завдання роботи. Метою роботи є розвиток та уточнення методів виявлення прихованих аналітичних структру, зокрема фейстель-подібних перетворень.

Для досягнення мети необхідно виконати такі завдання:

1) провести огляд опублікованих джерел за тематикою дослідження;

2) проаналізувати існуючі методи виявлення прихованих аналітичних структур в таблично заданих S-блоках;

3) Дослідити поведінку індикаторних матриць високого порядку структурованих криптографічних перетворень;

4) Узагальнити наявні методи виявленні на інші фейстель-подібні перетворення: схему $MISTY$, R-схему;

Об'єкт дослідження. Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предмет дослідження. Предметом дослідження є виявлення прихованих алгебраїчних структур у криптографічних перетвореннях.

Наукова новизна отриманих результатів. Вперше досліджено властивості індикаторних матриць високого порядку схеми $MISTY$ та R-схеми. На основі знайдених властивостей побудовано метод виявлення прихованих схем $MISTY$ або R-схем у таблично заданих S-блоках.

Практичне значення отриманих результатів. Результати даної роботи дозволяють уточнювати оцінки надійності для існуючих криптографічних перетворень та формувати вимоги щодо відкритих реалізацій криптоалгоритмів у моделі «white box».

Апробація результатів. Результати роботи були представлені на XI Міжнародній науково-практичній конференції «Інтернет-Освіта-Наука 2018» (м. Вінниця, 2018).

1 МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНИХ АНАЛІТИЧНИХ СТРУКТУР У КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕННЯХ

В даному розділі будуть подані необхідні терміни й позначення з теорії булевих функцій а також описані існуючі методи перевірки криптографічних перетворень на наявність прихованих аналітичних структур. Метод базується на визначенні залежності індикаторної матриці високого порядку від кількості раундів та алгебраїчного степеня раундової функції.

1.1 Булеві функції та їх властивості

Введемо терміни й поняття з теорії булевих функцій, які будуть нам необхідні. Докладніший опис булевих функцій та їх властивостей можна знайти в [1].

Визначення 1.1. Булева функція (одновимірна) - фунція, що відображає множину F_2^n в множину F_2. Функція, що відображає множину F_2^n в множину F_2^m називається векторною (багатовимірною) булевою функцією. Кожна багатовимірна булева функція може бути представлена у вигляді вектора одновимірних координатних функцій: $F = (f_1,\ldots,f_m)$.

Визначення 1.2. Збалансована булева функція (одновимірна) - булева фунція, що на всій своїй області визначення приймає значення 0 та 1 однакову кількість разів. Векторна булева функція називається збалансованою, якщо потужності прообразів для кожного її вихідного значення рівні між собою. Багатовимірна булева функція збалансована тоді й тільки тоді, коли кожна її координатна функція є збалансованою.

Визначення 1.3. Нехай $x = (x_0,\ldots,x_{n-1})$, $y = (y_0,\ldots,y_{n-1})$. Позначимо:

1) $x \cdot u = \bigoplus_{i=0}^{n-1} x_i \wedge y_i$

2) $\langle x, u \rangle$ - скалярний добуток векторів

3) $x^u = \prod_{i=0}^{n-1} x_i^{y_i}$

4) $x \preceq u$ виконується, якщо з того, що $u_i = 0$ завжди слідує $x_i = 0$, для всих $i \in [0, n-1]$. В такому випадку говорять, що u "покриває"x.

Визначення 1.4. Кожна одновимірна булева функція f може бути представлена у вигляді алгебраїчної нормальної форми (Algebraic Normal Form, ANF):

$$f(x) = \bigoplus_{u \in F_2^n} (a_u \cdot x^u),$$

де $a_u = \bigoplus_{x \preceq u}(f(x))$. Таке представлення є єдиним. Коефіцієнти a_u можуть бути знайдені за допомогою трансформації Мьобіуса. Для векторної булевої функції, її ANF буде набір ANF її координатних функцій.

Визначення 1.5. Алгебраїчна степінь булевої функції f- найбільша кількість змінних в термі ANF булевої фукнції. Алгебраїчна степінь векторної булевої функції F – максимальна алгебраїчна степінь її координатних функцій.

Визначення 1.6. Кожна одновимірна булева функція може бути представлена у вигляді ряду Фур'є:

$$f(x) = \sum_{a \in F_2^n} c_f(a) \cdot e^{i\pi\langle a,x \rangle},$$

де $c_f(a) = \frac{1}{2^n} \sum_{a \in F_2^n} f(x) \cdot e^{i\pi\langle a,x \rangle}$. Коефіцієнти $c_f(a)$ називають коефіцієнтами Фур'є булевої функції f, а множину $\{c_f(a) | a \in F_2^n\}$ - спектром Фур'є. Розклад у ряд Фур'є є однозначним, тому спектр повністю описує функцію f.

Визначення 1.7. Перетворення Уолша-Адамара булевої функції f називають перетворення такого виду:

$$W_f(a) = \sum_{a \in F_2^n} (-1)^{f(x) \oplus \langle a,x \rangle}$$

Відповідно, цілочисельні коефіцієнти $W_f(a)$ називають коефіцієнтами Уолша-Адамара (або просто коефіцієнтами Уолша) булевої функції, а їх множину – спектром Уолша.

Множина коефіцієнтів Уолша однозначно описує функцію f. Можна відновити f через обернене перетворення Уолша-Адамара:

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{a \in F_2^n} W_f(a) \cdot (-1)^{\langle a,x \rangle}$$

Визначення 1.8. Нелінійністю булевої функції f називається її відстань до класу лінійних функцій L_n, в термінах відстані Хемінга, тобто:

$$NL_f = min_{l \in L_n}(dist(f,l)) = min_{l \in L_n}(wt(f \oplus l))$$

Для нелінійності знайдено аналітичну оцінку із застосуванням коефіцієнтів Уолша:

$$NL_f = 2^{n-1} - \frac{1}{2} max_{l \in L_n} |W_f(a)|$$

1.2 Розпізнавання прихованих аналітичних структур в S-блоках

Наразі, одним із найпоширеніших різновидів криптографічного захисту інформації є симетричні блочні шифри. Вони оперують групами біт фіксованої довжини за допомогою симетричного ключа. Гарний, з точки зору стійкості до найбільш розповсюджених атак, шифр складається почергового комбінування лінійних і нелінійних перетворень й певної кількості раундів. Нелінійність забезпечується саме за допомогою шару S-блоків, які доволі часто використовуються при проектуванні блочних шифрів.

Визначення 1.9. S-блок (від англ. substitution box) –

відображення виду $S : \{0,1\}^n \to \{0,1\}^m$, яке використовується у блочних шифрах для забезпечення максимально складного зв'язку між бітами шифротексту, відкритого тексту та ключа. m та n не обов'язково рівні між собою.

Такі блоки називаються небієктивними (наприклад, S-блоки DES). При $m = n$, відповідні S-блоки називаються бієктивними (наприклад, S-блоки AES). Зазвичай $n = 8$, з міркувань ефективної апаратної і програмної реалізації.

Однією з найголовніших властивостей криптографічних S-блоків є стійкість до лінійного й диференціального криптоаналізу.

Визначення 1.10. Таблиця розподілів диференціалів (Difference Distribution Table, DDT) - матриця $||d_{ij}||$ розмірності $2^n \times 2^n$, де кожний елемент d_{ij} знаходиться за формулою:

$$d_{ij} = |\{x \in \{0,1\}^n | f(x \oplus i) \oplus f(x) = j\}|.$$

Часто нас цікавить максимальний елемент цієї матриці (без врахування першого рядка й першого стовпця) та кількість разів, скільки він зустрічається. Нехай $\Delta = max_{i>0,j>0}\{d_{ij}\}$. Диференційний криптоаналіз будується на основі пошуку пар (a,b) таких, що $f(x) \oplus f(x) = b$ має якомога більше розв'язків, що еквівалентно збільшенню величини d_{ab}. Тому з точки зору проектування S-блоків варто обирати такі, в яких Δ є якомога меншою.

Визначення 1.11. Таблиця розподілів лінійних апроксимацій (Linear Approximation Table, LAT) - матриця $||c_{ij}||$ розмірності $2^n \times 2^n$, де кожний елемент c_{ij} знаходиться за формулою:

$$c_{ij} = |\{x \in \{0,1\}^n | x \cdot i = f(x) \cdot j\}| - 2^{n-1} = \frac{1}{2} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot i \oplus f(x) \cdot j}.$$

Нас цікавить максимальний елемент цієї матриці (без врахування першого рядка й першого стовпця) та кількість разів, скільки він

зустрічається. Нехай $\lambda = max_{i>0,j>0}\{c_{ij}\}$. Для покращення криптографічних властивостей, обирають такі S-блоки, в яких величина λ є якомога меншою.

Окрім цього, S-блок можна розглядати як булеву функцію.

Питання вибору й побудови криптографічних S-блоків здавна турбувало фахівців. Постає проблема досягнення високої стійкості до криптоаналізу й відсутність явних аналітичних внутрішніх структур, які б дали змогу криптоаналітику отримати хоч якусь корисну інформацію.

На сьогодні відома велика кількість вдалих генераторів псевдовипадкових чисел і послідовностей, які застосовуються в багатьох областях криптографії і не тільки. Якщо використовувати тільки генератори псевдовипадкових чисел, то ймовірність отримати S-блок з гарними криптографічними властивостями доволі низька. Для прикладу був проведений експеримент: використовуючи відомий генератор Блюм-Блюма-Шуба (Blum Blum Shub, BBS) [2], за допомогою алгоритму Фішера-Йетса [3] було згенеровано S-блок з наступними характеристиками:

1) $\Delta = 12$, й зустрічається 2 рази.

2) $\lambda = 34$, й зустрічається 2 рази.

3) NL_f по кожній координатній функції відповідно дорівнюють: 106, 106, 100, 98, 104, 100, 100, 104.

З точки зору сучасного розвитку криптографії, цей S-блок не є надто надійним. Для прикладу візьмемо S-блок AES, про який відомо достовірно, що він вибраний не випадково, а аналітично, для підсилення його криптографічних властивостей. Для AES маємо:

1) $\Delta = 4$, й зустрічається 255 разів.

2) $\lambda = 16$, й зустрічається 1275 разів.

3) NL_f по кожній координатній функції відповідно дорівнюють: 112, 112, 112, 112, 112, 112, 112, 112.

Бачимо приклад надійного S-блоку. Взагалі існування S-блоку, в якому $\Delta = 2$, для $n = 8$ не доведено, тому даний S-блок можна вважати

одним із найкращих на сьогоднішній день. Сучасний розвиток електронно-обчислювальної техніки не дозволяє знайти подібний S-блок, використовуючи повний перебір, оскільки ймовірність випадково згенерувати подібну перестановку нехтовно мала. Тому для генерації стійких, з точки зору криптографії, блоків нині застосовують більш складні алгоритми. В результаті експерименту на генерацію одного S-блоку й обчислення необхідних параметрів було затрачено ≈ 3 секунди.

Оскільки ми з'ясували, що простого випадкового генерування недостатньо для отримання криптографічно стійких S-блоків, то часто для цього розробляють спеціальні алгоритми, за допомогою яких досягають бажаних результатів. Подібні алгоритми слід використовувати досить обережно й досліджувати окремо, оскільки вони можуть якось неявно вплинути на структуру блоку. В роботі [4] наведено теоретичні оцінки для певних статистичних параметрів випадкових S-блоків – зокрема, визначено теоретичну імовірність, що для випадкового S-блоку максимальне значення $\Delta(\lambda)$ таблиці DDT (LAT) буде зустрічатись не більше ніж N разів. За допомогою цих параметрів можна встановити, скільки необхідно перебрати випадкових S-блоків, щоб знайти S-блок із заданими параметрами [5].

Для DDT 8-бітного S-блоку відповідна імовірність оцінюється за такою формулою:

$$P(\Delta, N) = \sum_{l=0}^{N} C_{255^2}^{l} \cdot D(\Delta)^l \cdot (\sum_{d=0}^{\frac{\Delta}{2}-1} D(2d))^{255^2-l},$$

де $D(2d) = \frac{e^{-\frac{1}{2}}}{2^d d!}$ – імовірність розподілу Пуассона з параметром $\frac{1}{2}$.

Аналогічна формула для LAT має вид:

$$P(\lambda, N) = \sum_{l=0}^{N} C_{255^2}^{l} \cdot (L(\lambda) + L(-\lambda)) \cdot (\sum_{-\frac{\lambda}{2}+1}^{\frac{\lambda}{2}-1} L(2d))^{255^2-l},$$

де $L(2d) = \frac{(C_{128}^{64+d})^2}{C_{256}^{128}}$ – імовірність гіпергеометричного розподілу.

Відповідно, якщо ймовірність занадто низька, то доцільно висунути гіпотезу про те, що даний S-блок був обраний не випадковим чином. Наприклад, маємо, що максимальне значення DDT в S-блоці AES дорівнює 4 і зустрічається 255 разів. Тому $P(4, 255) \approx 10^{-2000}$, що фактично унеможлилює знаходження такї перестановки шляхом перебору. Для випадково обраного S-блоку, який був розглянутий вище, $P(4, 255) \approx 0.8$, що очевидно говорить про те, що даний S-блок міг бути обраний випадковим вибором із множини всіх перестановок за розумний час.

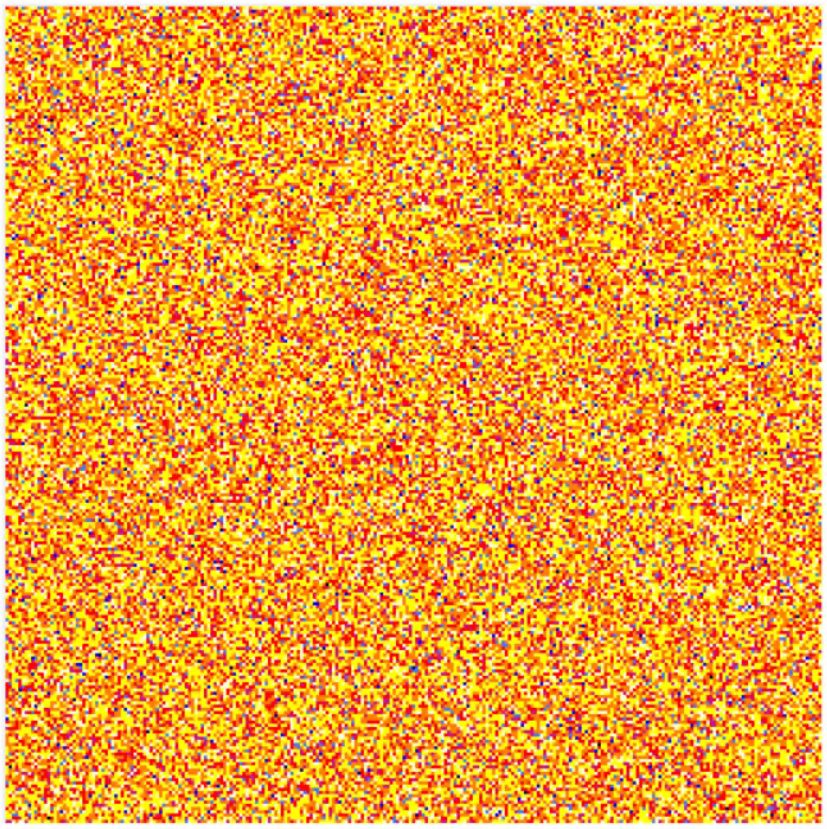

Рисунок 1.1 – Візуалізація методом Поллока випадкового S-блоку

Часто око людини може легко розрізнити внутрішні залежності виходячи тільки з візуального представлення. Принцип методу Поллока полягає в тому, щоб візуалізувати матрицю DDT або LAT, зафарбувавши на полотні відповідний піксель в залежності від відповідного йому коефіцієнту. Даний метод отримав назву в честь американського

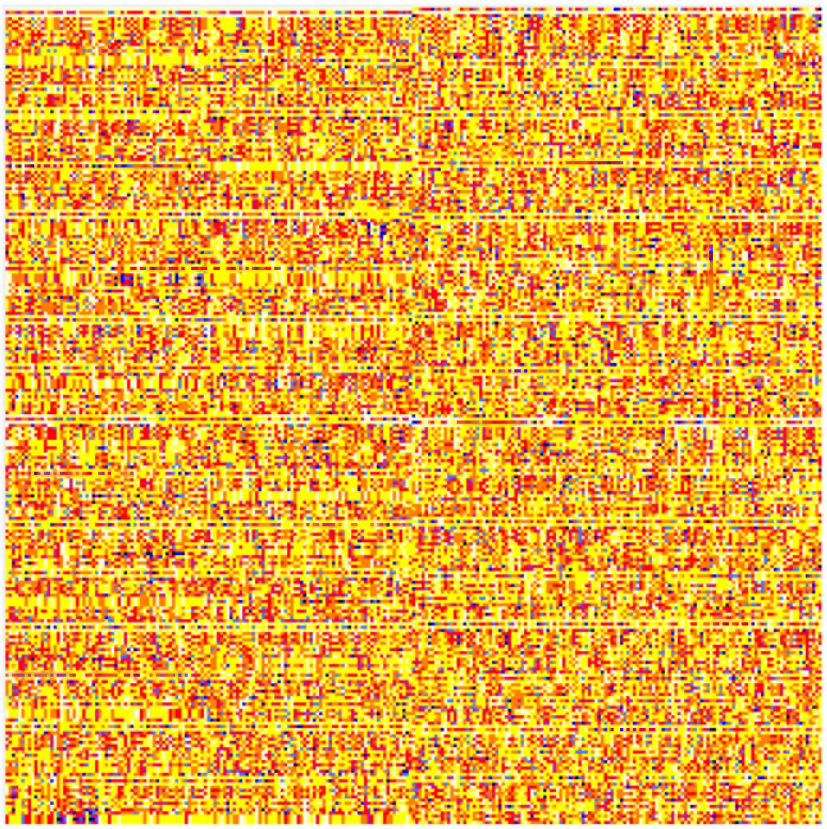

Рисунок 1.2 – Візуалізація методом Поллока S-блоку шифру SAFER

художника-експресіоніста Джексона Поллока, оскільки результат доволі часто схожий на його картини. Якщо S-блок був згенерований випадковим чином, візуалізація його DDT або LAT не матиме ніяких чітко окреслених структур. На рисунку 1.1 Зображена візуалізація методом Поллока таблиці LAT для S-блоку, що був розглянутий в розділі 1.2. Як видно, ніяких залежностей не помітно.

Розглянемо відомий шифр SAFER [6] . Про нього точно відомо, що S-блок, який в ньому використовується, не був обраний випадковим чином. Якщо поглянути на візуалізацію його таблиці LAT (рисунок 1.2), чітко проглядається «невипадкова» структура.

Окрім візуалізації DDT і LAT можна скористатися так званою $\oplus$ - текстурою.

Визначення 1.12. $\oplus$-текстурою таблиці розподілів лінійних апроксимацій L S-блоку будемо називати матрицю $T^{\oplus}$, коефіцієнти якої

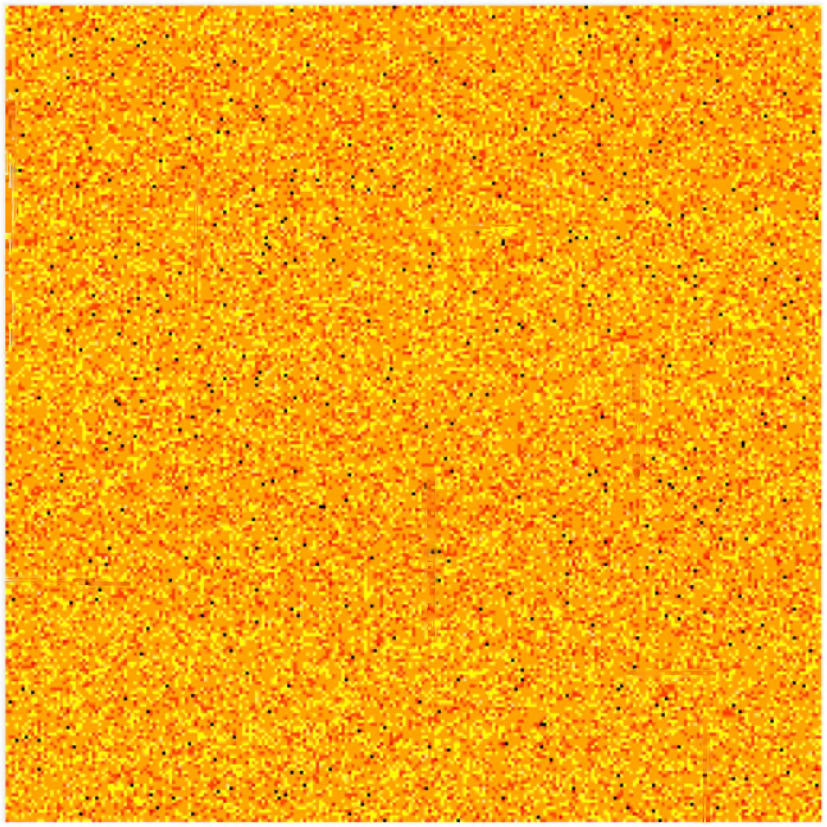

Рисунок 1.3 – Візуалізація методом Поллока $\oplus$-текстури випадкового S-блоку

визначаються за формулою:

$$T^{\oplus}[i,j] = |\{(x,y)||L[x \oplus i, y \oplus j]| = |L[x,y]|\}|$$

$\oplus$-текстура показує взаємну кореляцію між елементами LAT. Обраховану матрицю $T^{\oplus}$ також можна візуалізувати методом Поллока. Для випадкового S-блоку з розділу, візуалізація його $\oplus$-текстури зображена на рисунку 1.3.

Як видно, всі коефіцієнти виглядають доволі рівними, що свідчить про те, що в S-блоці нема ніяких внутрішніх залежностей. Якщо поглянути на візуалізацію $\oplus$-текстури S-блоку шифру SAFER (рисунок 1.4), то можна помітити неоднорідність зображення.

Аналогічно можна скористатися даним методом для візуалізації спектру Фур'є й Уолша. На рисунку 1.5 зображено розподіл коефіцієнтів для випадково згенерованого S-блоку. Синім зображені коефіцієнти

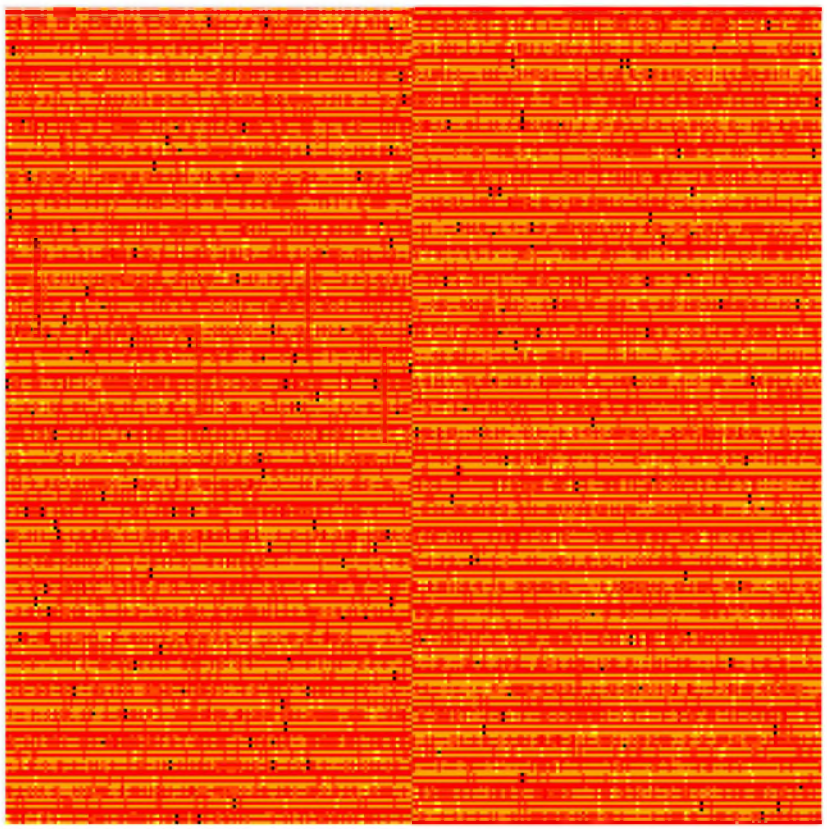

Рисунок 1.4 – Візуалізація методом Поллока $\oplus$-текстури S-блоку шифру SAFER

Фур'є, кожний з яких помножений на 2^8 (для зручності зображення). Червоним кольором зображені коефіцієнти Уолша. Нульове значення відмічає чорна лінія, якщо коефіцієнт від'ємний – він зображується нижче відміченого нульового значення, на відстані, що дорівнює його значенні за модулем, якщо ж більше – над чорною лінією.

Як видно, коефіцієнти розташовані рівномірно, що свідчить про відсутність внутрішніх прихованих структур, що можуть вплинути на будову S-блоку.

Розглянемо шифр «Zorro» [7]. Він також використовує 8-бітний S-блок, про який також відомо, що він був створений за допомогою детермінованого алгоритму, а не обраний випадковим чином. На рисунку 1.6 зображена візуалізація розподілу коефіцієнтів Фур'є й Уолша даного S-блоку. Помітні деякі періодичні скупчення в певних областях прямої, що свідчить про те, що даний S-блок має аналітичні залежності.

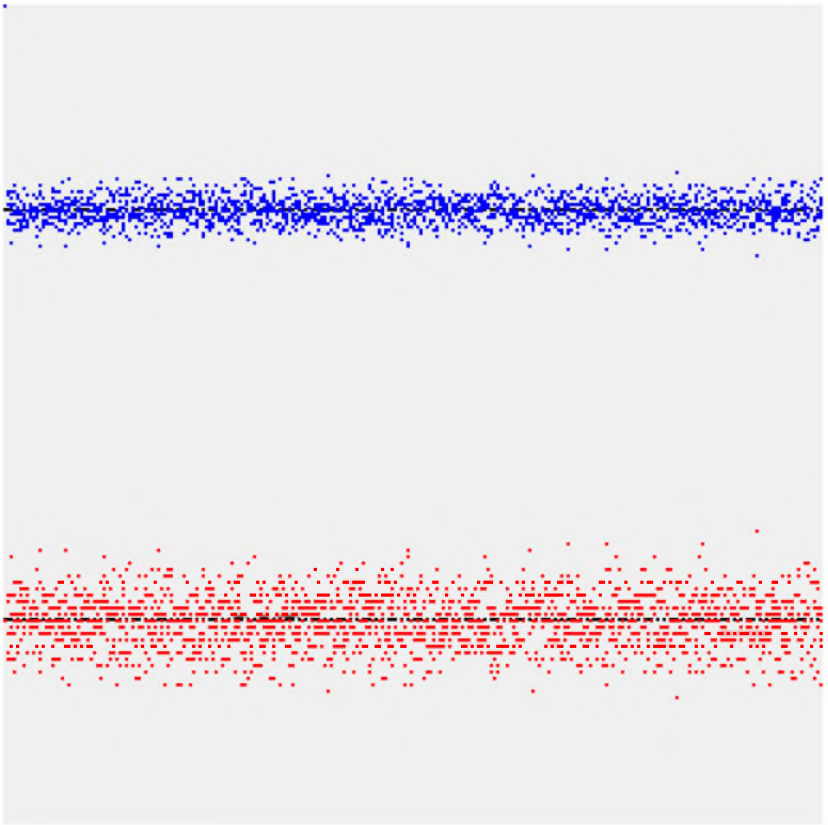

Рисунок 1.5 – Візуалізація розподілу коефіцієнтів Фур'є й Уолша випадкового S-блоку

В 2012 році в Російській Федерації було затверджено новий стандарт гешування «Стрибог» [8], а в 2015 році - новий 128-бітний блочний шифр «Кузнєчік» [9]. Обидва використовують один і той самий S-блок.

Автори стверджували, що він був згенерований випадковим чином. В статті [5] було доведено, що він має чітку аналітичну структуру. В приведеній статті покроково й детально описаний процес декомпозиції, в результаті чого був отриманий алгоритм, за яким розробники «Стрибогу» й «Кузнєчіка» спроектували S-блок.

Спершу було пораховано ймовірності випадкової генерації подібного S-блоку. Вони становили для DDT й LAT відповідно $2^{-82}, 2^{-40}$

Такі низькі ймовірності фактично виключають можливість вибору дано S-блоку шляхом перебору, адже на сьогодні обчислювальна техніка ще не досягла рівня, який би дозволив провести такі обчислення за розумний час. Автори прийшли до висновку, що подібний S-блоку був

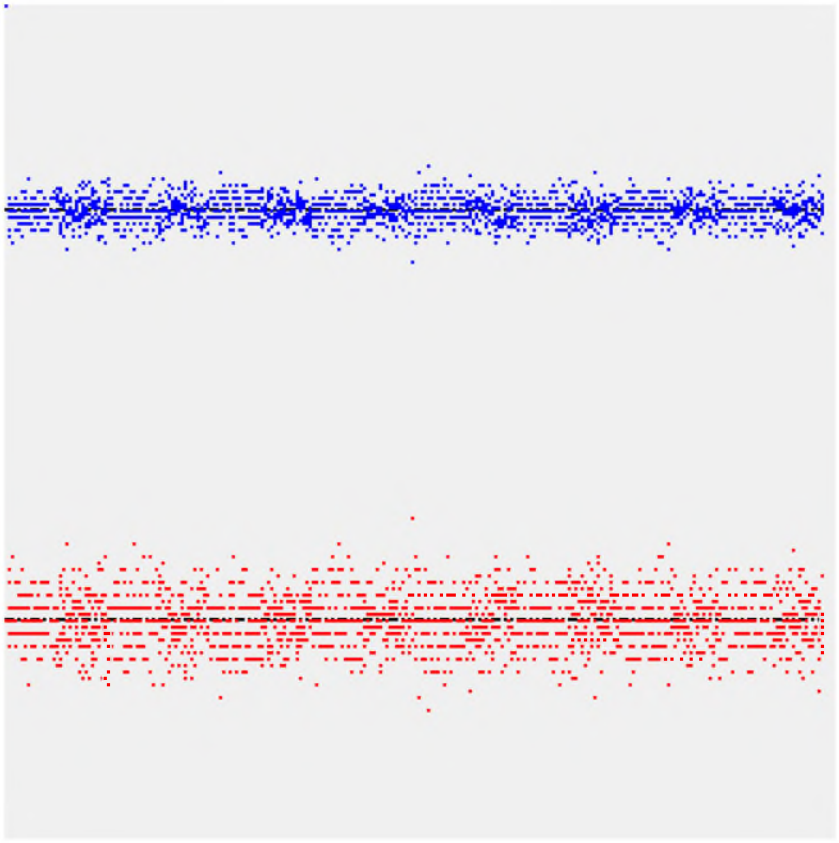

Рисунок 1.6 – Візуалізація розподілу коефіцієнтів Фур'є й Уолша S-блоку шифру Zorro

створений за допомогою аналітичних методів, які мали на меті покращення його диференціальних і лінійних властивостей.

В результаті був виведений алгоритм, за яким був отриманий S-блок шифру «Кузнєчік» та геш-функції «Стрибог». Питання про те, чого схема виглядає саме так і як обирались параметри залишається відкритим, як і те, як впливає подібна структура на стійкість S-блоку.

1.3 Індикаторна матриця високого порядку структурованих криптографічних перетворень

Аналогічних результатів хотілось би отримати, розглядаючи фейстель-подібні перетворення, адже на сьогодні вони також доволі часто

зустрічаються під час проектування сучасних криптосистем.

Будемо розглядати деяку фейстель-подібну схему, як чорний ящик, подаючи певні значення на вхід і отримуючи інші значення на виході. Першочерговою задачею буде виявлення природи внутрішньої структури такого перетворення й визначення, які це має наслідки для стійкості криптосистеми.

Твердження 1.1. *Нехай F - n-бітна перестановка, $(n > 2)$ й нехай L - її таблиця LAT. Тоді:*

$$\frac{L[a,b]}{2} = \bigoplus_{x \in F_2^n} (b \cdot F(x))(x \cdot x) \mod 2.$$

Введемо наступні позначення: $L_4[a,b] = L[a,b] \mod 4, L_4 \in \{0,2\}$, так як елементи $L[a,b]$ - парні.

Нехай:

$$B(L)[a,b] = \frac{L_4[a,b]}{2} = (\bigoplus_{x \in \{0,1\}^n} (b \cdot f(x))(a \cdot x)) \mod 2, B(L)[a,b] \in \{0,1\}$$

Визначення 1.13. Нехай F - n-бітна перестановка, $(n > 2)$, $B(L)$ - описана вище булева матриця для даної перестановки. Індикатора матриця високого порядку (High-Degree Indicator matrix, HDIM) $\hat{H}(F)$ - матриця розмірності $n \times n$, коефіцієнти якої обчислюються як:

$$\hat{H}(F)[i,j] = \bigoplus_{x \in \{0,1\}^n} (e_i \cdot F(x))(e_j \cdot x),$$

де e_k - нульовий вектор, у якого на місці k стоїть значення 1.

Виходячи з визначення, бачимо, що:

$$B(L)[i,j] = b^T \times \hat{H})(F) \times a.$$

Коефіцієнти матриці $\hat{H}(F)$ показують присутність найвищого степеня в координатних функціях F. Тобто $\hat{H}(F)[i,j] = 1$ тоді й тільки тоді, коли коли ANF координатної функції f_i містить многочлен степені

$n-1$ (має вигляд $\prod_{k \neq j} x_k$).

Складність обчислення такої матриці визначається як $O(n2^{n-1})$[10].

Використовуючи вищеописані терміни й визначення, поглянемо, як поводить себе HDIM на схемах Фейстеля (рисунок 1.7). Автори статті [10] пов'язують максимальну степінь d схеми Фейстеля й кількість раундів r з перевіркою наявносіт прихованих структур використовуючи функцію $\Theta : Z^2 \to Z$, яка обчислюється як:

$$\Theta(d, r) = d^{\lfloor \frac{r}{2} \rfloor - 1} + d^{\lceil \frac{r}{2} \rceil - 1}$$

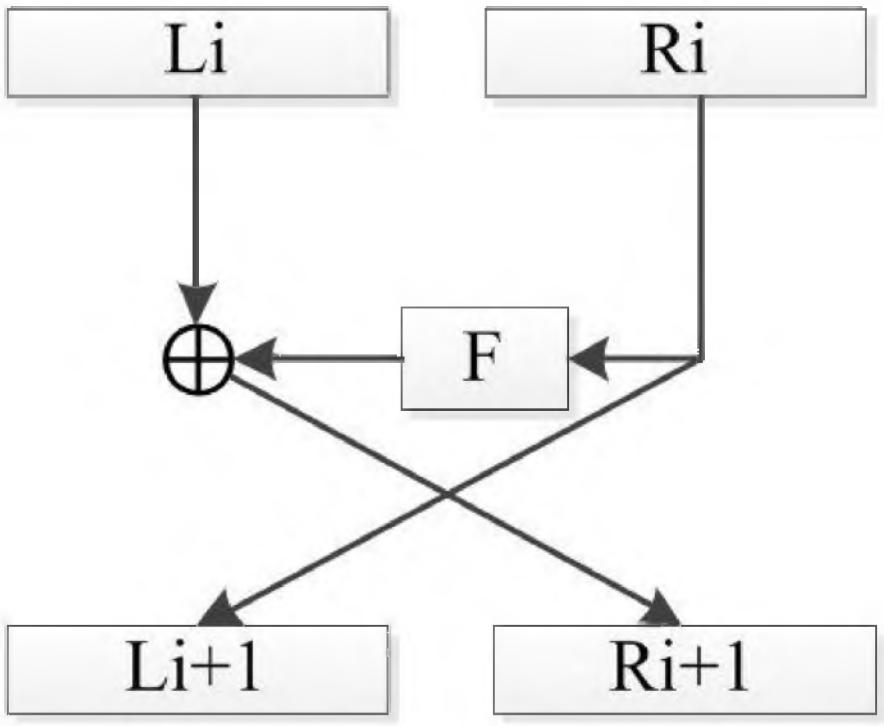

Рисунок 1.7 – Один раунд схеми Фейстеля

Сформуємо основну теорему[10], яка допомагає визначити внутрішню структуру схеми Фейстеля на основі обчислення HDIM.

Теорема 1.1. *Нехай F - $2n$-бітна схема Фейстеля, F_d^r, r - кількість раундів, $deg(f_i) \leq d$. Тоді $\hat{H}(F)[i,j] = 0$ при $i < n$ **та** $j < n$, якщо виконуються наступні умови:*

1) Якщо раундова функція біективна й $\Theta(d, r-1) < 2n$

2) Якщо раундова функціяне бієктивна й $\Theta(d,r) < 2n$

З теореми 1.1 можна сформувати наступний наслідок:

Наслідок 1.1. *Нехай* F *-* $2n$*-бітна схема Фейстеля,* F_d^r, r *- кількість раундів,* $deg(f_i) \leq d$*. Тоді* $\hat{H}(F)[i,j] = 0$ *при* $i < n$ ***або*** $j < n$*, якщо виконуються наступні умови:*

1) Якщо раундова функція бієктивна й $\Theta(d,r) < 2n$

2) Якщо раундова функціяне бієктивна й $\Theta(d,r+1) < 2n$

В процесі доведення теореми 1.1 автори статті [10] використовували наступну лему:

Лема 1.1. *Нехай* F *-* $2n$*-бітна перестановка, що має вигляд* $F : x \to F_l(x)||F_r(r)$*,* d *- кількість раундів,* $deg(f_i) \leq d$*. Нехай також* $G : x \to G_l(x)||G_r(r)$ *-* $2n$*-бітна перестановка, зокрема* $deg(G_r) = d_G$*,* $deg(G_l) \leq d \times d_G$*.*

Тоді $deg(F_l \circ G) \leq d^{r+1} \times d_G$*,* $deg(F_r \circ G) \leq d^r \times d_G$*.*

Формулювання даної леми буде узагальнено й доведено для інших фейстель-подібних перетворень в наступному розділі.

Для того, щоб проілюструвати вищеописану теорему й її наслідок, візьмемо 4-х й 5-и раундову схему Фейстеля з бієктивною 3-х бітною раундовою функцією, вибраною випадково й рівноймовірно. Раундова функція повинна мати степінь принаймні 2. Оскільки $\Theta(2,4) = 2^1 + 2^1 = 4 < 6$, тому HDMI даної схеми має структуру, описану в теоремі 2.

Справді:

$$\hat{H}(F^4) = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 0 & 1 \end{bmatrix}$$

$$\hat{H}(F^5) = \begin{bmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 1 & 1 & 1 \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Отже видно, що для досягнення високого степеня раундової функції був використаний певний сильно структурований метод. Даний метод можна ускладнити для знаходження виду многочленів найвищого степеня.

Висновки до розділу 1

В цьому розділі розглядалися методи, за допмогою яких можна певним чином визначити й проаналізувати внутрішню структуру деяких криптографічних перетворень, зокрема S-блоків та схем Фейстеля. На

прикладі декомпозиції стандарту шифрування «Кузнєчік» і гешування «Стрибог» Російської Федерації було продемонстровано практичну реалізацію описаних методів й показано, що S-блок не був вибраний випадковим чином.

Також був описаний новий математичний об'єкт - індикаторна матриця високого порядку (High-Degree Indicator matrix, HDIM). За допомогою цієї матриці було продемонстровано, як можна розпізнати приховане фейстелівське перетворення. Аналітично доведена теорема, яка показує зв'язок між кількісью раундів й степенем раундової функції та виглядом матриці HDIM.

В наступному розділі індикаторна матриця високого порядку буде побудована для інших фейстель-подібних перетворень, зокрема для схеми $MISTY$ та R-схеми й доведедені аналогічні теореми для цих перетворень.

2 МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНИХ ФЕЙСТЕЛЬ-ПОДІБНИХ ПЕРЕТВОРЕНЬ

В даному розділі буде показана залежність вигляду індикаторної матриці високого порядку від кількості раундів та алгебраїчного степеня раундової функції для фейстель-подібних перетворень.

2.1 Властивості алгебраїчних степенів Фейстель-подібних перетворень

Перед тим, як доведемо аналоги леми 1.1 для інших фейстель-подібних перетворень (а також обернених їм), сформулюємо ряд важливих тверджень.

Нехай F, G - деякі n-бітні перетворення, $deg(F) = d_1, deg(G) = d_2$; Тоді:

1) $deg(F \oplus G) \leq max(d_1, d_2)$

2) $deg(F(G)) = deg(G(F)) \leq d_1 \times d_2$

3) $deg(F||G) \leq max(d_1, d_2)$

В розділі буде розглянуто:

1) Схему $MISTY$ (рисунок 2.1):

Шифрування:

$$\begin{cases} L_{i+1} = R_i \\ R_{i+1} = F(L_i) \oplus R_i \end{cases}$$

Розшифрування:

$$\begin{cases} L_i = F^{-1}(R_{i+1} \oplus L_{i+1}) \\ R_i = L_{i+1} \end{cases}$$

Раундова функція F має бути бієктивною.Обернена схема не є схемою

$MISTY$ (рисунок 2.2).

2) R-схему (рисунок 2.3):

Шифрування:

$$\begin{cases} L_{i+1} = F(L_i) \oplus R_i \\ R_{i+1} = F(L_i) \end{cases}$$

Розшифрування:

$$\begin{cases} L_i = F^{-1}(R_{i+1}) \\ R_i = L_{i+1} \oplus R_{i+1} \end{cases}$$

Раундова функція F має бути бієктивною. Обернена схема не є R-схемою (рисунок 2.4).

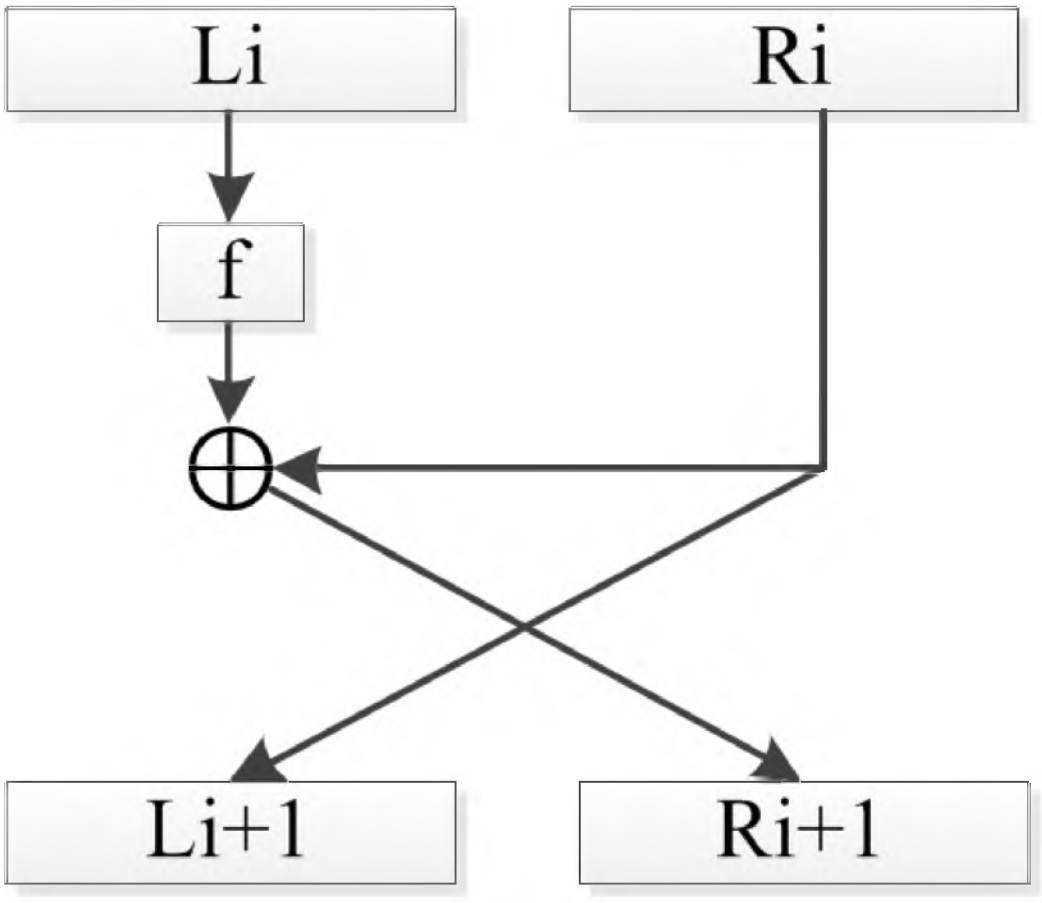

Рисунок 2.1 – Один раунд схеми $MISTY$

Лема 2.1. *Нехай F - $2n$-бітна схема $MISTY$, що має вигляд*

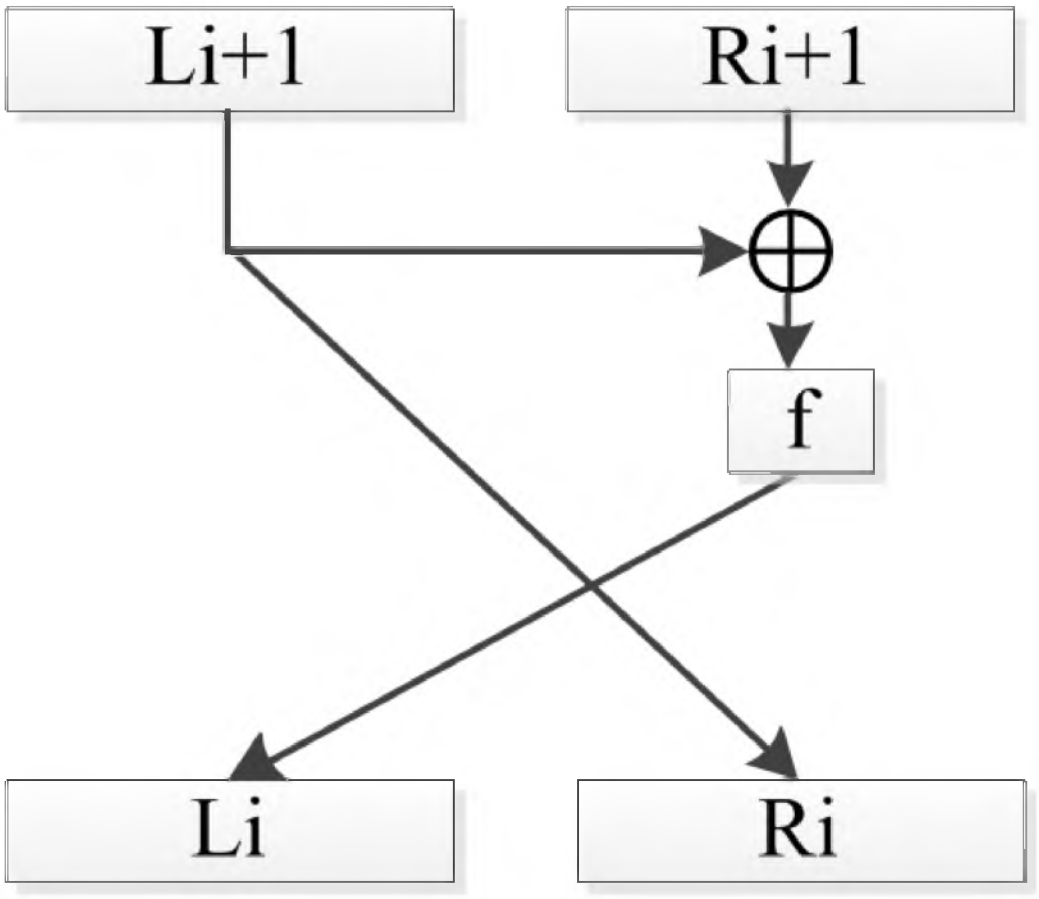

Рисунок 2.2 – Один раунд оберненої схеми $MISTY$

$F : x \to F_l(x)||F_r(r)$*(рисунок 2.1),* r *- кількість раундів,* $deg(f_i) \leq d$, $deg(F_l) = d_1, deg(F_r) = d_2$

Тоді:

1) $d_1 \leq d_2$, $d_2 \leq d_1 d$*:*

а) $r = 2k - 1$*:* $deg(F_l) \leq d_2 d^{\frac{r-1}{2}}$, $deg(F_r) \leq d_1 d^{\frac{r+1}{2}}$

б) $r = 2k$*:* $deg(F_l) \leq d_1 d^{\frac{r}{2}}$, $deg(F_r) \leq d_2 d^{\frac{r}{2}}$

2) $d_2 \leq d_1$*:*

а) $r = 2k - 1$*:* $deg(F_l) \leq d_1 d^{\frac{r-1}{2}}$, $deg(F_r) \leq d_1 d^{\frac{r+1}{2}}$

б) $r = 2k$*:* $deg(F_l) \leq d_1 d^{\frac{r}{2}}$, $deg(F_r) \leq d_1 d^{\frac{r}{2}}$

3) $d_1 \leq d_2$, $d_1 d \leq d_2$*:*

а) $r = 2k - 1$*:* $deg(F_l) \leq d_2 d^{\frac{r-1}{2}}$, $deg(F_r) \leq d_2 d^{\frac{r-1}{2}}$

б) $r = 2k$*:* $deg(F_l) \leq d_2 d^{\frac{r}{2}-1}$, $deg(F_r) \leq d_2 d^{\frac{r}{2}}$

Доведення.

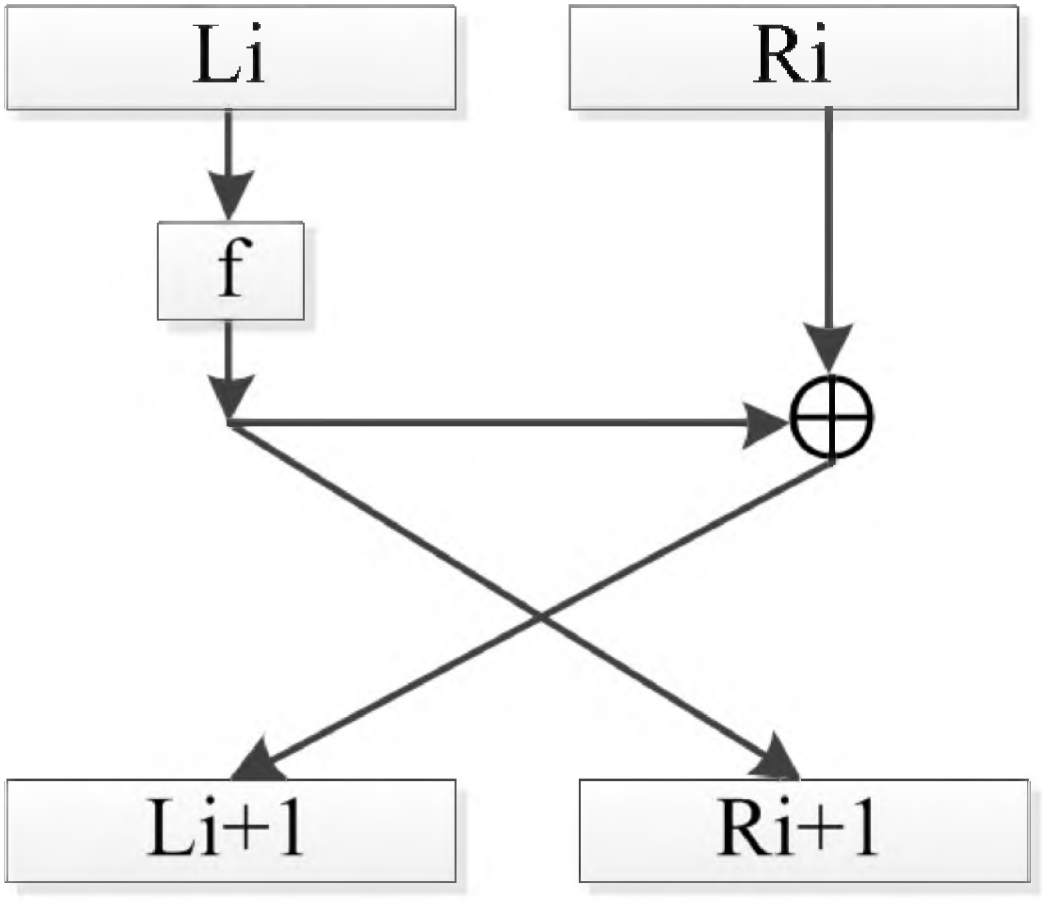

Рисунок 2.3 – Один раунд R-схеми

1) $d_1 \leq d_2$, $d_2 \leq d_1 d$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2$, $deg(F_r) \leq d_1 d$

б) $r = 2 : deg(F_l) \leq d_1 d$, $deg(F_r) \leq d_2 d$

в) $r = 3 : deg(F_l) \leq d_2 d$, $deg(F_r) \leq d_1 d^2$

г) $r = 4 : deg(F_l) \leq d_1 d^2$, $deg(F_r) \leq d_2 d^2$

д) $r = 5 : deg(F_l) \leq d_2 d^2$, $deg(F_r) \leq d_1 d^3$

Бачимо, що в загальному випадку це можна записати як:

а) $r = 2k - 1$: $deg(F_l) \leq d_2 d^{\frac{r-1}{2}}$, $deg(F_r) \leq d_1 d^{\frac{r+1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1 d^{\frac{r}{2}}$, $deg(F_r) \leq d_2 d^{\frac{r}{2}}$

2) $d_2 \leq d_1$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

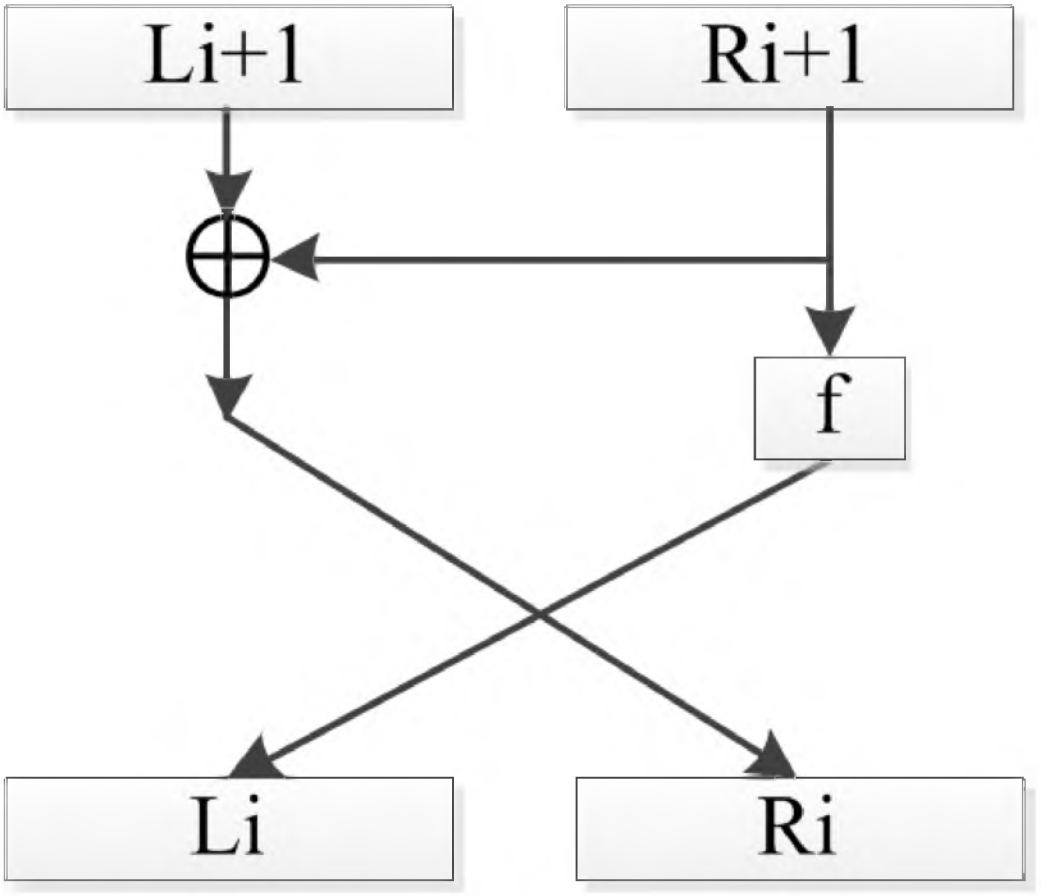

Рисунок 2.4 – Один раунд оберненої R-схеми

а) $r = 1 : deg(F_l) \leq d_2$, $deg(F_r) \leq d_1 d$

б) $r = 2 : deg(F_l) \leq d_1 d$, $deg(F_r) \leq d_1 d$

в) $r = 3 : deg(F_l) \leq d_1 d$, $deg(F_r) \leq d_1 d^2$

г) $r = 4 : deg(F_l) \leq d_1 d^2$, $deg(F_r) \leq d_1 d^2$

д) $r = 5 : deg(F_l) \leq d_1 d^2$, $deg(F_r) \leq d_1 d^3$

Бачимо, що в загальному випадку це можна записати як:

а) $r = 2k - 1$: $deg(F_l) \leq d_1 d^{\frac{r-1}{2}}$, $deg(F_r) \leq d_1 d^{\frac{r+1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1 d^{\frac{r}{2}}$, $deg(F_r) \leq d_1 d^{\frac{r}{2}}$

3) $d_1 \leq d_2$, $d_1 d \leq d_2$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2$, $deg(F_r) \leq d_2$

б) $r = 2 : deg(F_l) \leq d_2$, $deg(F_r) \leq d_2 d$

в) $r = 3 : deg(F_l) \leq d_2 d$, $deg(F_r) \leq d_2 d$

г) $r = 4 : deg(F_l) \leq d_2 d$, $deg(F_r) \leq d_2 d^2$

д) $r = 5 : deg(F_l) \leq d_2 d^2$, $deg(F_r) \leq d_2 d^2$

Бачимо, що в загальному випадку це можна записати як:

а) $r = 2k - 1$: $deg(F_l) \leq d_2 d^{\frac{r-1}{2}}$, $deg(F_r) \leq d_2 d^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_2 d^{\frac{r}{2}-1}$, $deg(F_r) \leq d_2 d^{\frac{r}{2}}$

□

Сформуємо й доведемо аналогічну лему для оберненої схеми $MISTY$.

Лема 2.2. *Нехай F - $2n$-бітна обернена схема $MISTY$, що має вигляд $F : x \to F_l(x)||F_r(r)$(рисунок 2.2), r - кількість раундів, $deg(f_i^{-1}) \leq \widetilde{d}$, $deg(F_l) = d_1, deg(F_r) = d_2$*

Тоді:

1) $d_1 \leq d_2$: $deg(F_l) \leq d_2 \widetilde{d}^r$ $deg(F_r) \leq d_2 \widetilde{d}^{r-1}$

2) $d_2 \leq d_1$: $deg(F_l) \leq d_1 \widetilde{d}^r$ $deg(F_r) \leq d_1 \widetilde{d}^{r-1}$

Доведення.

1) $d_1 \leq d_2$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2 \widetilde{d}$, $deg(F_r) \leq d_1$

б) $r = 2 : deg(F_l) \leq d_2 \widetilde{d}^2$, $deg(F_r) \leq d_2 \widetilde{d}$

в) $r = 3 : deg(F_l) \leq d_2 \widetilde{d}^3$, $deg(F_r) \leq d_2 \widetilde{d}^2$

г) $r = 4 : deg(F_l) \leq d_2 \widetilde{d}^4$, $deg(F_r) \leq d_2 \widetilde{d}^3$

д) $r = 5 : deg(F_l) \leq d_2 \widetilde{d}^5$, $deg(F_r) \leq d_2 \widetilde{d}^4$

Бачимо, що в загальному випадку це можна записати як: $deg(F_l) \leq d_2 \widetilde{d}^r$, $deg(F_r) \leq d_2 \widetilde{d}^{r-1}$

2) $d_2 \leq d_1$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_1 \widetilde{d}$, $deg(F_r) \leq d_1$

б) $r = 2 : deg(F_l) \leq d_1 \widetilde{d}^2$, $deg(F_r) \leq d_1 \widetilde{d}$

в) $r = 3 : deg(F_l) \leq d_1\widetilde{d}^3$, $deg(F_r) \leq d_1\widetilde{d}^2$

г) $r = 4 : deg(F_l) \leq d_1\widetilde{d}^4$, $deg(F_r) \leq d_1\widetilde{d}^3$

д) $r = 5 : deg(F_l) \leq d_1\widetilde{d}^5$, $deg(F_r) \leq d_1\widetilde{d}^4$

Бачимо, що в загальному випадку це можна записати як: $deg(F_l) \leq d_1\widetilde{d}^r$, $deg(F_r) \leq d_1\widetilde{d}^{r-1}$

□

Сформуємо й доведемо аналогічні леми для прямої й оберненої R-схеми.

Лема 2.3. *Нехай F - $2n$-бітна R-схема, що має вигляд $F : x \to F_l(x)||F_r(r)$(рисунок 2.3), r - кількість раундів, $deg(f_i) \leq d$, $deg(F_l) = d_1, deg(F_r) = d_2$*

Тоді:

1) $d_1 d \leq d_2$: $deg(F_l) \leq d_2 d^{r-1}$ $deg(F_r) \leq d_2 d^{r-1}$

2) $d_2 \leq d_1 d$: $deg(F_l) \leq d_1 d^r$ $deg(F_r) \leq d_1 d^r$

Доведення.

1) $d_1 d \leq d_2$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2$, $deg(F_r) \leq d_1 d$

б) $r = 2 : deg(F_l) \leq d_2 d$, $deg(F_r) \leq d_2 d$

в) $r = 3 : deg(F_l) \leq d_2 d^2$, $deg(F_r) \leq d_2 d^2$

г) $r = 4 : deg(F_l) \leq d_2 d^3$, $deg(F_r) \leq d_2 d^3$

д) $r = 5 : deg(F_l) \leq d_2 d^4$, $deg(F_r) \leq d_2 d^4$

Бачимо, що в загальному випадку це можна записати як: $deg(F_l) \leq d_2 d^{r-1}$, $deg(F_r) \leq d_2 d^{r-1}$

2) $d_2 \leq d_1 d$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_1 d$, $deg(F_r) \leq d_1 d$

б) $r = 2 : deg(F_l) \leq d_1 d^2$, $deg(F_r) \leq d_1 d^2$

в) $r = 3 : deg(F_l) \leq d_1 d^3$, $deg(F_r) \leq d_1 d^3$

г) $r = 4 : deg(F_l) \leq d_1 d^4$, $deg(F_r) \leq d_1 d^4$

д) $r = 5 : deg(F_l) \leq d_1 d^5$, $deg(F_r) \leq d_1 d^5$

Бачимо, що в загальному випадку це можна записати як: $deg(F_l) \leq d_1 d^r$, $deg(F_r) \leq d_1 d^r$

□

Лема 2.4. *Нехай F - $2n$-бітна обернена R-схема, що має вигляд $F : x \to F_l(x)||F_r(r)$(рисунок 2.4), r - кількість раундів, $deg(f_i^{-1}) \leq \widetilde{d}$, $deg(F_l) = d_1, deg(F_r) = d_2$*

Тоді:

1) $d_2 \leq d_1$, $d_1 \leq d_2\widetilde{d}$:

а) $r = 2k - 1$: $deg(F_l) \leq d_2\widetilde{d}^{\frac{r+1}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r}{2}}$, $deg(F_r) \leq d_2\widetilde{d}^{\frac{r}{2}}$

2) $d_2 \leq d_1$, $d_1 \leq d_2\widetilde{d}$:

а) $r = 2k - 1$: $deg(F_l) \leq d_2\widetilde{d}^{\frac{r+1}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r}{2}}$, $deg(F_r) \leq d_2\widetilde{d}^{\frac{r}{2}}$

3) $d_2 \leq d_1$, $d_2\widetilde{d} \leq d_1$:

а) $r = 2k - 1$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r}{2}-1}$

Доведення.

1) $d_2 \leq d_1$, $d_1 \leq d_2 d$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2\widetilde{d}$, $deg(F_r) \leq d_1$

б) $r = 2 : deg(F_l) \leq d_1\widetilde{d}$, $deg(F_r) \leq d_2\widetilde{d}$

в) $r = 3 : deg(F_l) \leq d_2\widetilde{d}^2$, $deg(F_r) \leq d_1\widetilde{d}^2$

г) $r = 4 : deg(F_l) \leq d_1\widetilde{d}^2$, $deg(F_r) \leq d_2\widetilde{d}^2$

д) $r = 5 : deg(F_l) \leq d_2\widetilde{d}^3$, $deg(F_r) \leq d_1\widetilde{d}^3$

Бачимо, що в загальному випадку це можна записати як:

а) $r = 2k - 1$: $deg(F_l) \leq d_2\widetilde{d}^{\frac{r+1}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r}{2}}$, $deg(F_r) \leq d_2\widetilde{d}^{\frac{r}{2}}$

2) $d_2 \leq d_1$, $d_1 \leq d_2 d$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2\widetilde{d}$, $deg(F_r) \leq d_1$

б) $r = 2 : deg(F_l) \leq d_1\widetilde{d}$, $deg(F_r) \leq d_2\widetilde{d}$

в) $r = 3 : deg(F_l) \leq d_2\widetilde{d}^2$, $deg(F_r) \leq d_1\widetilde{d}$

г) $r = 4 : deg(F_l) \leq d_1\widetilde{d}^2$, $deg(F_r) \leq d_2\widetilde{d}^2$

д) $r = 5 : deg(F_l) \leq d_2\widetilde{d}^3$, $deg(F_r) \leq d_1\widetilde{d}^2$

Бачимо, що в загальному випадку це можна записати як:

а) $r = 2k - 1$: $deg(F_l) \leq d_2\widetilde{d}^{\frac{r+1}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r}{2}}$, $deg(F_r) \leq d_2\widetilde{d}^{\frac{r}{2}}$

3) $d_2 \leq d_1$, $d_2 d \leq d_1$.

Запишемо степені лівої й правої частини при проходженні через перші декілька раундів схеми:

а) $r = 1 : deg(F_l) \leq d_2\widetilde{d}$, $deg(F_r) \leq d_1$

б) $r = 2 : deg(F_l) \leq d_1\widetilde{d}$, $deg(F_r) \leq d_1$

в) $r = 3 : deg(F_l) \leq d_1\widetilde{d}$, $deg(F_r) \leq d_1\widetilde{d}$

г) $r = 4 : deg(F_l) \leq d_1\widetilde{d}^2$, $deg(F_r) \leq d_1\widetilde{d}$

д) $r = 5 : deg(F_l) \leq d_1\widetilde{d}^2$, $deg(F_r) \leq d_1\widetilde{d}^2$

Бачимо, що в загальному випадку це можна записати як:

а) $r = 2k - 1$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r-1}{2}}$

б) $r = 2k$: $deg(F_l) \leq d_1\widetilde{d}^{\frac{r}{2}}$, $deg(F_r) \leq d_1\widetilde{d}^{\frac{r}{2}-1}$

□

2.2 Розпізнавання прихованих аналітичних структур в схемах $MISTY$

Поглянемо, який вигляд має HDIM в залежності від кількості раундів r й степеня d раундової функції f побудована на схемі $MISTY$.

Теорема 2.1. *Нехай F - $2n$-бітна схема $MISTY$, що має вигляд $F : x \to F_l(x)||F_r(r)$(рисунок 2.1), r - кількість раундів, $deg(f_i^{-1}) \leq \widetilde{d}$, $deg(f_i) \leq d$. Тоді $\hat{H}(F)[i,j] = 0$ якщо:*

1) $i < n$ при:

а) якщо $r = 4l+3$ та $\Theta = d^{l+1} + \widetilde{d}^{2l+1} < 2n$

б) якщо $r = 4l+2$ та $\Theta = d^{l+1} + \widetilde{d}^{2l} < 2n$

в) якщо $r = 4l+1$ та $\Theta = d^{l} + \widetilde{d}^{2l} < 2n$

г) якщо $r = 4l$ та $\Theta = d^{l} + \widetilde{d}^{2l-1} < 2n$

2) $0 < i < 2n$ при:

а) якщо $r = 4l+3$ та $\Theta = d^{l} + \widetilde{d}^{2l+1} < 2n$

б) якщо $r = 4l+2$ та $\Theta = d^{l} + \widetilde{d}^{2l} < 2n$

в) якщо $r = 4l+1$ та $\Theta = d^{l} + \widetilde{d}^{2l} < 2n$

г) якщо $r = 4l$ та $\Theta = d^{l} + \widetilde{d}^{2l-1} < 2n$

Доведення.

1) Спершу розглянемо випадок, коли $i < n$. Позначимо x_l, x_r - входи на перший раунд схеми, а y_l, y_r - виходи з останнього раунду. Нехай $r = 4l+3$, тобто кількість раундів можна поділити на дві частини по $2l+1$ й один раунд посередині. Нехай на вхід $k+1$-го раунду подаються дві невідомі константи a, b, $deg(a) = deg(b) = 1$.
В випадку, коли $i < n$, формула для HDIM має вигляд:

$$\hat{H}(F)[i,j] = \bigoplus_{a||b \in \{0,1\}^n} (e_i \cdot y_r(a,b))(e_j \cdot x_l(a,b) \oplus e_j \cdot x_r(a,b))$$

Позначимо $B(r) = deg(y_r) + deg(x_l||x_r)$. Обчислимо значення $deg(x_l), deg(x_r), deg(y_r)$, враховуючи що треба пройти $2l+1$ раунд

оберненої схеми $MISTY$ й $2l+1$ прямої.

Отримуємо: $deg(x_l) = \widetilde{d}^{2l+1}, deg(x_r) = \widetilde{d}^{2l}, deg(y_r) = d^{l+1}$. Тому $B(r) = d^{l+1} + max(\widetilde{d}^{2l+1}, \widetilde{d}^{2l}) \leq d^{l+1} + \widetilde{d}^{2l+1}$.

Перевіримо, тепер, який вигляд має HDIM при $0 < i < 2n$ й такому самому $r = 4l+3$. Тепер дещо змінюється вигляд HDIM:

$$\hat{H}(F)[i,j] = \bigoplus_{a||b \in \{0,1\}^n} (e_i \cdot y_l(a,b))(e_j \cdot x_l(a,b) \oplus e_j \cdot x_r(a,b))$$

Відповідно, $B(r)$ тепер має вигляд $B(r) = deg(y_l) + deg(x_l||x_r) \leq d^l + max(\widetilde{d}^{2l+1}, \widetilde{d}^{2l}) \leq d^l + \widetilde{d}^{2l+1}$.

Аналогічно проводиться доведення теореми й для інших випадків r.

□

Бачимо, що матриця може бути повністю заповнена нулями при виконанні деяких умов. Це може слугувати певним індикатором при перевірці перестановки на наявність внутрішніх структур.

2.3 Розпізнавання прихованих аналітичних структур в R-схемах

Поглянемо, який вигляд має HDIM в залежності від кількості раундів r й степеня d раундової функції f побудована на R-схемі.

Теорема 2.2. *Нехай F - $2n$-бітна R-схема, що має вигляд $F : x \to F_l(x)||F_r(r)$(рисунок 2.1), r - кількість раундів, $deg(f_i^{-1}) \leq \widetilde{d}$, $deg(f_i) \leq d$. Тоді $\hat{H}(F)[i,j] = 0$ якщо:*

1) $i < n$ при:

а) якщо $r = 4l+3$ та $\Theta = d^{2l+1} + \widetilde{d}^{l+1} < 2n$

б) якщо $r = 4l+2$ та $\Theta = d^{2l+1} + \widetilde{d}^{l} < 2n$

в) якщо $r = 4l+1$ та $\Theta = d^{2l} + \widetilde{d}^{l} < 2n$

г) якщо $r = 4l$ та $\Theta = d^{2l} + \widetilde{d}^{l} < 2n$

2) $0 < i < 2n$ *при:*

а) якщо $r = 4l + 3$ *та* $\Theta = d^{2l+1} + \widetilde{d}^{l+1} < 2n$

б) якщо $r = 4l + 2$ *та* $\Theta = d^{2l+1} + \widetilde{d}^{l} < 2n$

в) якщо $r = 4l + 1$ *та* $\Theta = d^{2l} + \widetilde{d}^{l} < 2n$

г) якщо $r = 4l$ *та* $\Theta = d^{2l} + \widetilde{d}^{l} < 2n$

Доведення.

1) Спершу розглянемо випадок, коли $i < n$. Позначимо x_l, x_r - входи на перший раунд схеми, а y_l, y_r - виходи з останнього раунду. Нехай $r = 4l + 3$, тобто кількість раундів можна поділити на дві частини по $2l + 1$ й один раунд посередині. Нехай на вхід $k + 1$-го раунду подаються дві невідомі константи a, b, $deg(a) = deg(b) = 1$.

В випадку, коли $i < n$, формула для HDIM має вигляд:

$$\hat{H}(F)[i,j] = \bigoplus_{a||b \in \{0,1\}^n} (e_i \cdot y_r(a,b))(e_j \cdot x_l(a,b) \oplus e_j \cdot x_r(a,b))$$

Позначимо $B(r) = deg(y_r) + deg(x_l||x_r)$. Обчислимо значення $deg(x_l), deg(x_r), deg(y_r)$, враховуючи що треба пройти $2l + 1$ раунд оберненої схеми $MISTY$ й $2l + 1$ прямої.

Отримуємо: $deg(x_l) = \widetilde{d}^{l+1}, deg(x_r) = \widetilde{d}^{l}, deg(y_r) = d^{2l+1}$. Тому $B(r) = d^{2l+1} + max(\widetilde{d}^{l+1}, \widetilde{d}^{l}) \leq d^{2l+1} + \widetilde{d}^{l+1}$.

Перевіримо, тепер, який вигляд має HDIM при $0 < i < 2n$ й такому самому $r = 4l + 3$. Тепер дещо змінюється вигляд HDIM:

$$\hat{H}(F)[i,j] = \bigoplus_{a||b \in \{0,1\}^n} (e_i \cdot y_l(a,b))(e_j \cdot x_l(a,b) \oplus e_j \cdot x_r(a,b))$$

Відповідно, $B(r)$ тепер має вигляд $B(r) = deg(y_l) + deg(x_l||x_r) \leq d^{2l+1} + max(\widetilde{d}^{l+1}, \widetilde{d}^{l}) \leq d^{2l+1} + \widetilde{d}^{l+1}$.

Аналогічно доводиться й для інших випадків r.

□

Тобто, $\hat{H}(F)[i,j] = 0$ при виконанні умов теореми, при чому це не залежить від парності величини r(як у попередньому варіанті) Отже це

також може слугувати індикатором присутності даного Фейстель-подібного перетворення при його дослідженні.

Доведені теореми показують, що при невеликих значеннях d й r можливо розпізнати внутрішню структуру деякого перетворення, якщо воно було побудоване за допомогою фейстель-подібного перетворення. Зокрема, якщо індикаторна матриця високого порядку повністю заповнена нулями, то можна висунути припущення, що в основі її будови лежить R-схема.

Тому, при проектуванні криптосистем на базі фейстель-подібних перетворень необхідно звертати увагу на степінь раундової функції (а також функції, оберненої до неї), щоб уникнути випадків, коли умови вищеописаних теорем виконуються й можуть видати криптоаналітику певну інформацію про внутрішню структуру криптосистеми.

Висновки до розділу 2

В цьому розділі аналітично були сформовані й доведені теореми, які дозволяють виявляти внутрішню Фейстель-подібну структуру невідомих перетворень. Розпізнавання таких структур базується на обчисленні індикаторної матриці високого порядку, яка залежить від кількості раундів та степені раундової функції.

В результаті вдалося сформувати критерії, на основі яких можна висовувати припущення про внутрішню структуру перетворень, а саме, що вони можуть бути побудовані на основі Фейстель-подібних схем.

ВИСНОВКИ

У роботі було розглянуто методи виявлення та розпізнавання аналітичних структур в різних фейстель-подібних перетвореннях. Коротко викладено основні математичні означення, які лежать в основі описаних методів.

Розглянуто, який вигляд має індикаторна матриця високого порядку для схем $MISTY$ та R-схем в залежності від кількості раундів та алгебраїчного степеня раундової функції. Також показана залежність алгебраїчного степеня раундової функції фейстель-подібних перетворень від кількості раундів. Така залежність знадобилась для доведення основних теорем про структуру індикаторної матриці високого порядку. Показано, що для R-схеми, при невеликих значеннях параметрів r та d індикаторна матриця високого порядку повністю заповнена нулями.

З отриманих результатів зроблено висновок, що Фейстель-подібні перетворення можуть бути ідентифіковані за допомогою облислення індикаторної матриці високого порядку.

Наразі невідомо, як поводять себе індикаторні матриці високого порядку інших структурованих перетворень, які не були розглянуті в даній роботі, оскільки універсального алгоритму розпізнавання подібних структур наразі не існує.

ПЕРЕЛІК ПОСИЛАНЬ

1. Carlet, C.: Boolean functions for cryptography and error correcting codes. Boolean Models and Methods in Mathematics, Computer Science, and Engineering 2 (2010) 257–397.

2. Blum, Lenore; Blum, Manuel; Shub, Mike (1 May 1986). "A Simple Unpredictable Pseudo-Random Number Generator". SIAM Journal on Computing 15 (2): 364–383.

3. Fisher, R.A.; Yates, F. Statistical tables for biological, agricultural and medical research. — 3rd. — London: Oliver Boyd, 1948. — P. 26–27.

4. J. Daemen, V. Rijmen. Probability distributions of correlation and diffrentials in block ciphers // Journal of Mathematical Cryptology. – №1(3). – 2007.

5. A. Biryukov, L. Perrin and A. Udovenko. Reverse-Engineering the SBox of Streebog, Kuznyechik and STRIBOBr1 (Full Version). – 2016.–http://eprint.iacr.org/2016/071.

6. J.L .Massey. Safer k-64: A byte-oriented block-ciphering algorithm. In: Fast Software Encryption, Springer (1994) 1 – 17.

7. B. Gérard, V. Grosso, M. Naya-Plasencia, F.X. Standaert. Block ciphers that are easier to mask: how far can we go? In: Cryptographic Hardware and Embedded Systems-CHES 2013. Springer (2013) 383 – 399.

8. Federal Agency on Technical Regulation and Metrology: GOST R 34.11-2012: Streebog hash function (2012) https://www.streebog.net/.

9. V. Shishkin, D. Dygin, I. Lavrikov, G. Marshalko, V. Rudskoy, D. Trifonov.Low-weight and hi-end: Draft Russian Encryption Standard. CTCrypt'14, 05-06 June 2014, Moscow, Russia. Preproceedings (2014) 183–188.

10. L. Perrin, A. Udovenko. Algebraic Insights into the Secret Feistel Network (Full Version). – 2016.–http://eprint.iacr.org/2016/398.